UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/630,711	08/01/2000	Bjorn Markus Jakobsson	3037-4196	7518

7590 08/24/2005

Morgan & Finnegan LLP
345 Park Avenue
New York, NY 10154-0053

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/630,711	JAKOBSSON ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 6/6/05.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-28 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-28 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 28 September 2000 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 6 June 2005.

2. Claims 1-28 are pending in the application.

3. Claims 1-28 have been rejected.

Response to Arguments

4. Applicant's arguments with respect to claims 1-23 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

5. Claim 4 is objected to because of the following informalities: antecedent basis. Appropriate correction is required.

Claim 4 recites the limitation "said security goal" in the claim. There is insufficient antecedent basis for this limitation in the claim. For the sake examining, the examiner assumes that claim 4 depends upon claim 2.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-4 are rejected under 35 U.S.C. 102(e) as being anticipated by Banker et al U.S. Patent No. 6,005,938.

As to claim 1, Banker et al discloses distributing a computational task among a plurality of entities for execution within a specified interval of time as a POW [column 4, lines 37-53]. Banker et al discloses receiving the POW relating to the task from one of the plurality of entities. Banker et al discloses using the POW to accomplish the task [column 5, lines 6-62].

As to claim 2, Banker et al discloses using the POW to accomplish a security goal [column 5, lines 6-62].

As to claim 3, Banker et al discloses distributing the task among a plurality of entities includes partitioning the task into a plurality of sub-computational tasks and distributing each one of the plurality of sub-computational tasks to a respective one of the plurality of entities [column 5 line 64 to column 6 line 27].

As to claim 4, Banker et al discloses that the security goal involves restricting resource access by the one of the plurality of entities [column 6, lines 28-54].

7. Claims 5-7, 12-15, 17 and 23 are rejected under 35 U.S.C. 102(e) as being anticipated by Geer, Jr. et al U.S. Patent No. 6,212,634 B1.

As to claims 5 and 13, Geer, Jr. et al discloses partitioning a minting operation into a plurality of sub-computational tasks [column 3 line 55 to column 4 line 56]. Geer, Jr. et al discloses distributing one of the plurality of sub-computational tasks to one of a plurality of entities [column 3 line 55 to column 4 line 56]. Geer, Jr. et al discloses receiving a POW from the one of the plurality of entities. Geer, Jr. et al discloses using the POW to accomplish the minting operation [column 3 line 55 to column 4 line 56].

As to claims 6 and 14, Geer, Jr. et al discloses using the POW to accomplish a security goal [column 3 line 55 to column 4 line 56].

As to claims 7, 12 and 15, Geer, Jr. et al discloses that the minting operation includes identifying valid solutions that hash to a predetermined image. Geer, Jr. et al discloses that the POW represents a valid solution [column 5 line 52 to column 6 line 3].

As to claim 17, Geer, Jr. et al discloses that the predetermined number of valid solutions hash to a portion of the target value [column 5 line 52 to column 6 line 3].

As to claim 23, Geer, Jr. et al discloses verifying the POW [column 5 line 52 to column 6 line 3].

8. Claims 24-28 are rejected under 35 U.S.C. 102(e) as being anticipated by Frankel et al U.S. Patent No. 6,237,097 B1.

As to claim 24, Frankel et al discloses a method of using a computational effort invested in a proof of work (POW), comprising:

> generating a computational task for a certain amount of intense computation in a specified period of time as a POW to accomplish a separate, useful and verifiable correct computation [column 10, lines 38-48];
>
> distributing the computational task for execution among a plurality of server entities receiving a POW relating to said task from one of said plurality of said server entities [column 10 lines 49-67]; and
>
> using said POW to verify and accomplish said computational task [column 10 lines 49-67].

As to claim 25, Frankel et al discloses that the proof of work POW is (w, p) hard if prover P with memory resources bounded by m performs an average, over al coin flips by P and V, of at most w steps of computation in the time interval [ts,tc], and the verifier V accepts the probability at most p+o(m/poly(l)), where l is a security parameter; ts is start time and tc is complete time [column 12 line 51 to column 13 line 29].

As to claim 26, Frankel et al discloses that a proof of work POW is (w,p,m) feasible if there exists a prover P with memory resources bounded by m such that with an average of w steps of computation in the time interval [ts, tc], the prover can cauls the verifier V to accept with probability at least p [column 13 line 60 to column 14 line 19].

As to claim 27, Frankel et al discloses that a proof of work POW is sound, if, for some w, POW is (w,l,poly (l)) feasible, where l is a security parameter [column 13 line 60 to column 14 line 19].

As to claim 28, Frankel et al discloses that a POW may be regarded as efficient if the verifier performs substantially less computation than the prover [column 14 line 37 to column 15 line 22].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 8, 9 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Geer, Jr. et al U.S. Patent No. 6,212,634 B1 as applied to claim 5 above, and further in view of Van Hook et al U.S. Patent No. 6,549,210 B1.

As to claims 8 and 9, Geer, Jr. et al does not teach that the predetermined image comprises a range of images. Geer, Jr. et al does not teach that all images within the range of images have a predetermined number of least significant bits in common.

Van Hook et al teaches hashing that has predetermined image that comprises a range of images [column 9, lines 56-67]. Van Hook et al teaches that all images within the range of images have a predetermined number of least significant bits in common [column 11, lines 13-25].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Geer, Jr. et al so that the hashing would have had a predetermined image that comprises a range of images. All images within the range of images would have had a predetermined number of least significant bits in common.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Geer, Jr. et al, as discussed above, by the teaching of Van Hook et al because it reduces the likelihood that adjacent addresses will map to the same cache regions. The hashing process is optimized to be sensitive to small changes in the input data so that similar sets of input data will preferably not result in the same or even similar output data [column 7, lines 15-28].

As to claim 11, Geer, Jr. et al teaches that the security goal involves restricting resource access [column 6, lines 8-26].

10. Claims 10 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Geer, Jr. et al U.S. Patent No. 6,212,634 B1 as applied to claims 5 and 13 above, and further in view of Xiao U.S. Patent No. 6,662,167 B1.

As to claim 10, Geer, Jr. et al does not teach that each of the sub-tasks comprises searching a different solution search space for valid solutions.

Xiao teaches sub-tasks comprising searching a different solution search space for valid solutions [column 2, lines 26-53].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Geer, Jr. et al so that each of the sub-tasks would have comprises searching a different solution search space for valid solutions.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Geer, Jr. et al, as discussed above, by the teaching of Xiao because it produces a near-optimal or optimal sequence of products for manufacture [column 1, lines 13-17]

11. Claims 16 and 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Geer, Jr. et al U.S. Patent No. 6,212,634 B1 as applied to claim 13 above, and further in view of Simon U.S. Patent No. 5,768,385.

As to claims 16 and 19-21, Geer, Jr. et al does not teach that the privacy is maintained in the minting operation by keying the hash function with a secret value. Geer, Jr. et al does not teach that the secret value includes a portion specific to a coin. Geer, Jr. et al does not teach that the secret value includes a portion specific to a period of the coin's validity.

Simon teaches that the privacy is maintained in a minting operation by keying the hash function with a secret value. Simon teaches that a secret value includes a portion specific to a coin [column 8 line 65 to column 9 line 15]. Simon teaches that a secret value includes a portion specific to a period of the coin's validity [column 9 line 61 to column 10 line 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Geer, Jr. et al so that privacy was maintained in a minting operation by keying the hash function with a secret value. The secret value would have included a portion specific to a coin. The secret value would have included a portion specific to a period of the coin's validity.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Geer, Jr. et al, as discussed above, by the teaching of Simon because it combines the features of physical cash (privacy, anonymity, unforgeability) with the best features of electronic commerce (speed, ease and potential security of transport and storage) [column 1, lines 6-31].

12. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Geer, Jr. et al U.S. Patent No. 6,212,634 B1 as applied to claim 13 above, and further in view of Puhl et al U.S. Patent No. 5,768,385.

As to claim 22, Geer, Jr. et al does not teach that the hash is of a concatenation of a solution and a value generated using the secret value.

Puhl et al teaches hashing a concatenation of a solution and a value generated using the secret value [column 17, lines 24-42].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Geer, Jr. et al so that a concatenation of a solution and a value generated using the secret value would have been hashed.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Geer, Jr. et al, as discussed above, by the teaching of Simon because it thwarts theft of services and cloning [column 1, lines 24-31].

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy AM
August 18, 2005

Primary Examiner
AU2131
8/19/05